VZCZCXYZ0695
RR RUEHWEB

DE RUEHFR #1361/01 2790647
ZNY SSSSS ZZH
R 060647Z OCT 09
FM AMEMBASSY PARIS
TO RUEHC/SECSTATE WASHDC 7286
INFO RUEHZL/EUROPEAN POLITICAL COLLECTIVE
RUEKJCS/SECDEF WASHINGTON DC

S E C R E T PARIS 001361

STATE FOR T, PM, EUR/WE and EEB/CBA
SECDEF FOR DTSA

NOFORN
SIPDIS

E.O. 12958: DECL:09/24/19
TAGS: ETTC PARM PREL ETRD EUN FR
SUBJECT: END-USE ASSURANCES: FRANCE'S PERSPECTIVE ON THIRD PARTY TRANSFER

CLASSIFIED BY EMIN SETH WINNICK FOR REASONS 1.4 B & D

REFS: A) BRUSSELS 1238
B) PARIS 0872
C) FRENCH EMBASSY WASHINGTON NOTE VERBALE NO. 737
D) LISTON-RUETER EMAIL SENT 4/9/2009 5:02 PM (NOTAL)

¶1. (S) SUMMARY AND ACTION REQUEST: Several major allied military systems, including Belgium's A400M military air transport project (ref A), have been delayed for months, pending GOF end-user assurances (EUA). GOF will now provide necessary EUA in these cases, based on a previously existing bilateral commitment to the U.S. to account for certain encryption items on its territory. However, the broader issue of a European Union that will soon treat its national markets as a single "trusted community," in which sensitive technology can be transferred with a single European license (see ref B), is increasingly at odds with U.S. export control laws and regulations. Post recommends that Washington agencies engage with the European Commission and member states to find ways to bridge what will be a growing gap between our respective export control systems. In the interim, Embassy recommends Department review closely and respond to the confidential April 8, 2009 Note Verbale from the French Embassy in Washington (ref C) and clarify whether it satisfies EUA requirements for all/all transfers of covered encryption items to France. END SUMMARY AND ACTION REQUEST.

Major Allied Defense Systems Held Up by EUA Issue

¶2. (S) The French government regularly signs end-use assurances (EUA) to the USG when France is the end-user of sensitive or arms-related items. It has refused, however, to give such assurances for controlled items ultimately destined for systems outside France, in the absence of a government-to-government framework agreement. This has led to delays in a number of major European defense projects impacting both U.S. exporters and defense cooperation interests as well as French defense contractors. The United Kingdom's Future Strategic Tanker Aircraft (FSTA) program as well as A400M military air transport projects in Luxembourg, Belgium and Spain have been delayed many months pending GOF EUA for Thales France, one of several key firms involved in these programs.

The French Position

¶3. (S/NF) The senior MOD export control coordinator has told Embassy Paris that the GOF has no problem with signing EUA's for items or technical data for which it is the end-user. When the end-user is a foreign or private entity, the GOF's view is that it is not in a position to provide a meaningful end-use assurance because the GOF is not a party to the contract; and because the GOF does not have mechanisms or legal authority to ascertain or control the whereabouts of all ITAR items within its territory. The GOF considers EUAs the responsibility of the contracting/sub-contracting party, barring a government-to-government agreement.

An Unauthorized Lapse

¶4. (S/NF) In 2006, Paris learned that a former French defense cooperation attach in Washington was signing EUAs for temporary third-party transfer to private entities in France without authorization. This practice was then stopped. According to the MOD, the only such temporary EUAs it has been asked to sign related to encryption, but the USG never specified the limits, or extent, of the EUA requirement. Under these circumstances, the GOF suspended the signing of all EUA's where the GOF is not the end-user.

Government-to-Government Framework Offer a Solution

¶5. (S/NF) GOF export control officials have told us that one way around the GOF's lack of legal authority to provide EUAs is if the items in question are covered by a government to government agreement. Under a 1999 NSA Memorandum of Agreement with its French counterpart, the SCSSI, the GOF put in place mechanisms to track and assure secure storage and non-transfer of all NSA-designated encryption items in its territory, regardless of end-use. In a March 20, 2009 internal review of the EUA request related to the UK's FTSA program, the Prime Minister's office committed to finding a way to allow the UK program to go forward. On April 8, the French Embassy in Washington provided PM/RSAT with a diplomatic note confirming that the 1999 MOA covers transfer of cryptographic components and confirming GOF end-use assurances for such items. MOD contacts state that the GOF has not received a response to this note.

¶6. (S) As in the Belgian case (ref A), the FTSA case involved Multifunctional Info Distribution System (MIDS) cryptographic chipsets, manufactured in the United States. The GOF position is that all encryption items covered by the 1999 MOA (not just for the FTSA, as mentioned in the dipnote) have GOF end-use assurance and

require no further GOF documentation. Post request Department's clarification on whether the April 8 note satisfies EUA requirements for all third-party transfers of encryption items in France, or just MIDS chipsets, or only the MIDS chipsets in the FTSA.

Broader Issue of Integrated European Defense Industry

¶7. (S) Although the immediate problem of EUAs for temporary transfers to France involving encryption may be solved, the broader question of an increasingly integrated European defense industry -- and a European export control system that treats it as such - presents the USG with a growing challenge. On the margins of the June 2009 Paris Air Show (ref B), GOF and industry representatives noted that the European Base for Industrial and Technological Defense will be based upon "global licenses" that rely on common EU criteria that national government authorities will use to certify companies (for up to five years). However, no "global end use assurance" exists for re-export by one purchaser to another member of the "EU trusted community", a concept the USG does recognize. A/DAS for Defense Trade Robert S. Kovac raised with GOF and industry officials concerns on procedures to remove a company or country from the EU "trusted community." It was unclear how effective liaison and coordination among member states would occur.

¶8. (S) The GOF also recognizes a need for better coordination on export control practices. MOD officials have told us they favor focusing on a limited number of "highly sensitive" items such as encryption. GOF export control officials have told us, however, that the GOF does not desire to be held accountable for all/all ITAR items temporarily transferred to private parties in France.

COMMENT

¶9. (S) The armaments industry and the European Union have evolved so that cases of temporary third-party transfer during systems production are increasingly common. It is likely that the absence of French (or other) end-use assurances for non-encryption items will block or delay future allied defense projects which may be of substantial commercial and security interest to the U.S. Thus, while we may have a possible solution for encryption items, Embassy has had no success in engaging the GOF in a process to address end-use assurances for other ITAR items destined for third parties. We recommend Washington agencies engage with their French and EU counterparts on agreements or other appropriate ways to prevent

significant EUA-related delays in future allied defense systems. End Comment.

RIVKIN